Date: 1/2/01 Express Mail Label No. EL552572135US

Inventor(s): Edward D. English, Dana B.Whitney,
Rolland Zeleny and William L. Burke

Attorney's Docket No.: 1517.1008-002

DATA FLOW CONTROL UNIT

RELATED APPLICATIONS

This application is a continuation-in-part of and claims priority to U.S. Application No. 09/595,152 filed June 16, 2000, which itself claims the benefit of prior U.S. Provisional Application Serial Number 60/139,986 filed on June 18, 1999, entitled "Access Control Lock," the entire teachings of both of which are incorporated herein by this reference.

BACKGROUND

Many computer-related applications incorporate some level of security to restrict user access. For example, in many applications, it is often necessary that a user of a computer provide a password to log on to a computer and corresponding network. The use of a password provided by a user affords at least some level of protection against intruders that would otherwise tamper with a computer and its contents.

Although the use of a password can be advantageously incorporated in many applications, there are sometimes

drawbacks associated with their use. For instance, a user can forget a password if it is not used for an extended period of time. In some cases, a user can forget his or her password after returning from a long vacation.

To make matters worse, some systems require a user to change the password on a periodic basis for heightened security. This only adds to the difficulty of keeping track of a password at any given time. Even if a password is written on a piece of paper for later reference, the paper can be easily lost or destroyed, thwarting its purpose.

A password is also easily replicated to the extent that it can be transferred from one person to another by word of mouth. Thus, if a hacker breaks into a computer system and retrieves a user's password, this key is easily passed on to other vandals who can then tamper with a computer system and its contents. Moreover, a user that is assigned a password can misplace his or her trust in a friend who carelessly reveals a password to others even though it was intended to be kept secret.

These potential drawbacks are particularly disturbing since a corporation's most valuable asset is quite often information accessible by a user logging onto a password-protected computer.

SUMMARY OF THE INVENTION

The present invention is generally an apparatus and method for regulating data flow of information based on a position of a key in a lock assembly. More particularly, an illustrative embodiment of the present invention includes a mechanical lock that is activated by turning a key to an enabling or disabling position. Depending on a

position of the key in the lock assembly, an electronic circuit enables a flow of data to a target network.

In certain applications, the data information transmitted to a target address is intercepted and decoded to identify whether the data information includes a request for data such as a web page available on a network. If so, the data information is further transmitted to the target address on the network based upon a position of the key in the lock assembly. More specifically, the data information including a request for data located on the network is transmitted to a target circuit if the key in the lock assembly is turned to an enabling position. Accordingly, access of information such as web page information through a communication link can be controlled by an administrator of a network having a key to the lock assembly by switching the key to an appropriate position.

A flow of data information can also depend on a provided password in conjunction with a position of the key in a corresponding lock assembly. For example, data information can be blocked if an appropriate password is not provided by a user attempting to transmit the data information. Alternatively, a flow of data information can depend on whether a user turning the key in the lock assembly provides a proper password for enabling or disabling data flows through a data or communication link.

A data base is optionally provided to store a set or multiple sets of data flow rules for determining which data information is allowed to flow through a communication link to a target address on a network. In conjunction with a position of the key in a lock assembly, the data flow rules dictate the conditions in which data

is allowed to flow. For example, the key can potentially be set to one of multiple positions, enabling a corresponding mode of operation and set of data rules. Based on a selected mode, the corresponding set of data flow rules is used to determine which data information is allowed to pass to a corresponding target destination. Thus, different users can be allowed different levels of access to information on the network based on a position of the key in the lock assembly.

In a more specific application incorporating the principles of the present invention, the data information includes data packets such as TCP/IP (Transmission Control Protocol/Internet Protocol) packets and is decoded to determine whether the data information includes a URL (Uniform Resource Locator) indicating from which website data is to be retrieved or accessed. If the data information includes a request for access of information on a target network, the data information including the request is further transmitted to a target destination depending on a position of the key in the lock assembly and the data flow rules corresponding to the position of the key. In this way, it is possible to limit access of a user generating the data information from accessing information on a network. For example, in cases where the request for data information is blocked from a target destination, a corresponding user is unable to retrieve information from certain web sites as dictated by a selected set of data flow rules. In a similar manner, the data information can be decoded to determine the IP (Internet Protocol) address to which the data information is transmitted to selectively block the retrieval of certain information from a network.

In a similar application as previously described, the data information is generated by a user at a computer on a first network and the data information is transmitted to a target address on a second network. For example, the first network can be a local area network of multiple users or clients and the second network can be the Internet supporting access to a target address such as a network server on the Internet. Consequently, the position of the key in the lock assembly and data flow rules can be defined so that access to information on the target network is limited based on, for instance, which user is requesting access, the time of day or week, an allowed list of web sites, or type of communication session established by a particular user.

One way to sense the position of the key in the lock assembly is to couple the lock assembly to a switch and sense the state of the switch. Multiple switch positions, *i.e.*, more than two, can be provided to support multiple access modes, where each position of the switch corresponds to a selected access mode and set of data flow rules that is to be used for regulating data flows. Different keys fitting the key-way of the lock assembly can be cut so that certain keys enable a key holder to set the switch to a limited number of positions, allowing a key-holder to select only certain access modes. Some keys can be cut so that a corresponding key-holder can turn the key in a corresponding lock assembly to select one of any of the possible access modes.

This aspect of the present invention is advantageous in applications where the communication link is coupled to a computer that is shared by multiple users. For example, each user can be issued a key enabling a corresponding

user to select an appropriate access mode and retrieve information on a network.

In addition to limiting access to a network, the principles of the present invention can be used to block other types of data information. For example, an E-mail message directed to a target address on a network can be blocked from further transmission based upon a position of the key in the lock assembly. Thus, it is possible to restrict a user from transmitting potentially sensitive data such as secret corporate information to unauthorized recipients.

The present invention has many other advantageous features over the prior art. Specifically, a key-holder activating the lock assembly can control access of one or multiple users on a single computer or network of computers by switching the lock assembly to a desired switch position. Thus, data flows on, for example, a common traffic route can be regulated based upon an operational mode as selected by a position of a key in a lock assembly.

Many computer-related applications utilize a password such as a string of ASCII characters that are input through a keyboard to restrict user access. In such cases, an expert hacker can unfortunately break software codes to determine a password and, to the dismay of the system administrator, tamper with a computer and its contents. It is unlikely that such a software hacker is equally trained at the art of picking locks. Hence, the security system of the present invention is difficult to bypass for many vandals. Although a password provides some level of protection against intruders and is valuable in certain applications, once a password is revealed, it

can be relayed to other users by word of mouth whereas a physical key can be replicated only by a skilled craftsman.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other objects, features and advantages of the invention will be apparent from the following more particular description of preferred embodiments of the invention, as illustrated in the accompanying drawings in which like reference characters refer to the same parts throughout the different views. The drawings are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention.

Fig. 1 is a block diagram illustrating the interconnectivity of various components for regulating data flows according to the principles of the present invention.

Fig. 2 is a diagram of an exemplary switch coupled to a lock assembly according to the principles of the present invention.

Fig. 3 is a table including data flow rules for regulating a flow of data information according to the principle of the present invention.

Fig. 4 is a block diagram illustrating the interconnectivity of various components for regulating data flows from a single computer according to the principles of the present invention.

Fig. 5 is a flow chart indicating an exemplary process for regulating data flows according to the principles of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

A description of preferred embodiments of the invention follows.

Fig. 1 is a block diagram of a communication system 100 incorporating a data flow control unit 130 for regulating a flow of data information through a data link according to the principles of the present invention. As shown, data flow control unit 130 is disposed to regulate a flow of data information between terminal equipment. For example, data information generated by a user at terminal device 110 is transmitted to a remote device 160. In a reverse direction, data information generated at remote device 160 is transmitted to any or all terminal devices 110-1, 110-2, ... 110-n. Based on a position of key 132 in lock assembly 133, flows of data information are regulated. Thus, according to the principles of the present invention, a key-holder can control access of one or multiple users at corresponding terminal devices 110 by switching the key 132 in the lock assembly 133 to an enabling or disabling position.

In an application of the present invention where only a key 132 is necessary to select how data information is regulated as selected by a position of the key 132 in the lock assembly 133, an operator need not remember a password that can be easily forgotten or lost. For example, even if a password is written on a piece of paper, it is easily destroyed or copied. A physical key 132, preferably made of metal, for selecting an operational mode of data flow control unit 130 can be retained on a key ring and is much less likely than a password to be lost, copied or destroyed. Thus, there is a diminished likelihood that a key 132 will end up in the

hands of an individual that will wrongly use system 100. Additionally, it is likely that a system administrator in possession of the key 132 carries a key chain for other personal items, so it is not necessarily inconvenient for him or her to also carry a key 132 for selecting an operational mode of data flow control unit 130.

Certain environments do not lend themselves to safely provide a keyboard and display for supporting the input of a password to select an operational mode of data flow control unit 130. For example, if the data flow control unit 130 is located in an environment susceptible to vandalism, a mere lock assembly 133 that supports selectivity of data flow modes is much less likely to be destroyed or tampered with than a keyboard and display that often spur more interest to a passer-by. A keyboard and display can also be very costly to support even if they are properly protected from vandals. Thus, whether a keyboard and display are additionally provided for selecting an operational mode of data flow control unit 130 depends on a particular application.

Many applications utilize a password such as a string of ASCII characters to restrict user access or mode selectivity. Although this level of security is advantageous in many situations, a drawback associated with a system based solely on a provided password is that an expert hacker can sometimes break software codes to determine the password and, to the dismay of the system administrator, tamper with a computer and its contents. It is unlikely that such a software hacker is equally trained at the art of picking locks. Hence, the security system of the present invention is more difficult to bypass. Although a password provides some level of

protection against intruders, once a password is revealed, it can be relayed to other users by word of mouth whereas a physical key can be replicated only by a skilled craftsman.

In the exemplary embodiment as shown, data flow control unit 130 includes a communication controller 136 disposed between first link 125 and second link 145 to intercept the data flow of information between terminal devices 110 and remote devices 160. Communication controller 136 is coupled to memory 138 that stores a set of data flow rules 140 for regulating the flow of data information. Additionally, communication controller 136 is coupled to key position sensor 134 that detects a position of key 132 in lock assembly 133.

Fig. 2 is a diagram illustrating additional details of key position sensor 134. A voltage source 210 and pull-up resistor 220 produce position signal 200 that is fed to communication controller 136. The position signal 200 reflects the state of switch 222 coupled to lock assembly 133. Switch lever 225 is electrically conductive and is coupled to switch position signal 200. Based upon a position of the key 132 in lock assembly 133, switch lever 225 is generally set to either position A 240 or position B 230.

While switch lever 225 is in position A 240, position signal 200 is pulled down to ground 250. Conversely, while switch lever 225 is set to position B 230, switch position signal 200 is pulled up by voltage source 210. In this way, communication controller 136 senses the state of switch 222 and, therefore, the position of setting of key 132 in lock assembly 133 based upon a status of position signal 200. This key-controlled system can be

very inexpensive to produce, especially compared to the cost of a keyboard and display that are often required in applications supporting password-controlled systems.

Although only a two-position switch 222 is shown in Fig. 2 as described above, key position sensor 134 can include a lock assembly 133 and switch 222 supporting multiple positions. For example, referring again to Fig. 1, key 132 can be used to select mode A, B, C, D or E as shown, where each switch position corresponds to a different access mode. Of course, this configuration requires slightly more complex circuitry than a two-position switch. This can be achieved using multiple pull-up resistors. Specifically, a pull-up resistor for each mode can be provided so that communication controller 136 can detect when key 132 is set to one of multiple positions. Accordingly, communication controller 136 can sense a key-selected mode of operation of data flow control unit 130.

In the two-position switch as described, communication controller 136 senses the setting of a two-position switch 222 supporting, for example, a locked and unlocked mode corresponding to position A 240 and position B 230, respectively. While in an unlocked position, data information through data flow control unit 130 is passed on to an intended target destination without restrictions. Conversely, while in a locked position data information is not necessarily allowed to flow to a target address. Of course, which mode is selected based upon a given switch position is arbitrary. For instance, data flows can be completely blocked while the key 132 is in the locked position and restricted in an unlocked position.

Referring again to Fig. 1 as previously discussed, another aspect of the present invention includes providing a set of data flow rules that dictate which data information shall be blocked or passed to a target address depending on a selected mode of operation. For example, consider a case where a user at terminal device 110-1 transmits data information such as TCP/IP data packets to a remote device 160 such as a network server on the Internet. The data information is transmitted through link 115-1 to first communication link 125 to communication controller 136 that intercepts the data information. Based on a position of the key 132 and data flow rules corresponding to a selected mode of operation, the intercepted data information is either blocked or further transmitted to second communication link 145 through network 150 such as the Internet to a remote device 160. Communication controller 136 can include a buffer such as a FIFO device (First In First Out) to temporarily store data information as it is being processed.

Although in the exemplary application data information is transmitted as TCP/IP data packets, information can be transmitted based on other communication protocols. It also should be noted that data information can be transmitted from remote device 160 to a terminal device 110.

In a similar manner as previously discussed, data information transmitted in the reverse direction is optionally intercepted by communication controller 136, where it is either blocked or further transmitted to a target terminal device 110-1, 110-2, ..., 110-n. Depending on an application and corresponding data flow

rules, data information transmitted through data flow control unit 130 can be regulated in either or both directions.

When data flows are regulated in a reverse direction, system 100 is similar to a firewall. Firewalls are security systems intended to protect an organization's network against external threats from vandals such as hackers. In many applications, firewalls prevent computers in one network system from communicating directly with computers in another network system and vice versa. Instead, communications are routed to a proxy that determines whether it is safe to pass the information through to the organization's network. According to the principles of the present invention, communication controller 136 functions similar in many respects to a proxy server that regulates data flows. However, in the present application, data flows are regulated depending on a position of a key 132 in a corresponding lock assembly 133. That is, different levels of firewall protection are achieved by selecting a corresponding operational mode using key 132.

In one application, data flow control unit regulates data flows based on a position of the key 132 in lock assembly 133 and a provided password 170. For example, to select a particular mode of operation, in addition to selecting a switch position by turning the key 132 in lock assembly 133, an operator can provide a password 170. Although not shown, a user can type in such a password 170 on a keyboard coupled to a display device. This provided password 170 can then be compared to a list stored in communication controller 136. Accordingly, confirmation of password 170 as input by an operator provides an

additional level of security to insure that the operator selecting the operational mode of data flow control unit 130 via key 132 has the authority to do so. This added level of security insures that the operator has the authority to regulate data flows, which can be vitally important to the security of, for example, corporate information.

As previously mentioned, terminal devices 110 can be part of a LAN (Local Area Network). For example, each terminal device 110 can be connected to communication controller 136 through communication links 125 and 115. The links 115 and 125 connecting terminal devices 110 to communication controller 136 are preferably an Ethernet-type link based on the IEEE 802.3 standard. Alternative link-types such as those based on SNA (Systems Network Architecture), ARC net IEEE 802.5 (Token Ring), FDDI (Fiber Distributed Data Interface), Local Talk, ARCnet (Attached Computer Resources network), HPNA (Home Phone Networking Alliance), HomeRF (Home Radio Frequency), Home Plug (Home Plug Powerline Alliance), Bluetooth, or any other standard can be used to communicate information according to the principals of the present information.

Another standard for providing connectivity between terminal devices 110 and communication controller 136 is IEEE 802.11, which is a standard for WLANs (Wireless Local Area Networks). In short, the 802.11 standard describes a protocol for transmitting data among multiple transceivers (not shown) over a wireless link.

The 802.x standards generally provide access to channels based on an access method known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). In simple terms, this method is based on a "listen before

talk" scheme. For example, a transceiver located in each terminal device 110 and communication controller 136 monitors traffic on a radio channel to determine if another transceiver is transmitting. If the radio channel is clear, the terminal device 110 can transmit information over the radio channel. Based on this CSMA/CA scheme, transmission of data from the same transmitter cannot occur before a minimum time gap. After the minimum time gap has passed, the station selects a random "backoff interval" which is the wait time before the radio channel is again monitored to determine whether the radio channel is clear to transmit. If the channel is still busy, a shorter backoff interval is selected. This process is repeated until the transmitter is allowed to transmit data.

Network messages or data information transmitted by a transceiver device over a wireless link typically include an extra protocol layer so that packets can be transmitted over the radio channel and, thereafter, be processed by a transceiver device at communication controller 136 upon receipt. Once received, the extra protocol layer is stripped off to retrieve the original network messages for further processing as previously discussed. In a reverse direction, network messages emanating from communication controller 136 destined for one of the terminal devices 110 are reformatted before transmission over the exemplary wireless communication link 100. As in the former mentioned implementation of data flows from a terminal device 110 to communication controller 136, an extra layer added by a transceiver at communication controller 136 in the reverse direction is likewise stripped off by receiving terminal devices 110. In short, the extra

wireless protocol layer is used to reformat network messages, facilitating the transmission of such data over a wireless communication link.

Further details of the aforementioned standard of transmitting data information can be found in IEEE 802.11, which is available from IEEE located in Princeton, New Jersey. Likewise, the IEEE 802.3 standard related to Ethernet communication is also available from the IEEE.

It should be noted that the use of IEEE 802.11 compliant equipment is merely exemplary. Other wireless or hardwired systems can be used to support communication among a plurality of terminal devices 110 and communication controller 136.

Fig. 3 is a table of an illustrative set of data flow rules according to the principles of the present invention. As previously mentioned, each operational mode of data flow control unit 130 utilizes a different set of data flow rules. For example, the position of key 132 in lock assembly 133 dictates an operational mode of data flow control unit 130 and which set of data flow rules 140 are selected for regulating data flows.

In one application, the data flow control unit 130 regulates data information based upon contents of the data information. More specifically, flows can be regulated depending on a content of a data packet and embedded information indicating a user or terminal device 110 transmitting the data information. One way to determine a source of data information is to include such information in the data information and detect it at the data flow control unit 130 as it is intercepted. For example, a TCP/IP data packet includes a source address indicating from which terminal device 110 a data packet of

information is transmitted. Once it is known from which device the data information is transmitted as a result of processing corresponding data, the data information can be disposed of accordingly. That is, the data information can be transmitted to a target destination according to corresponding data flow rules 140. The data information can also be blocked from a target destination.

As mentioned, data flow rules 140 can dictate different conditions under which a particular user or terminal device 110 is allowed to transmit and receive data information through data flow control unit 130. One aspect of regulating data flows is based on a session type selected for communicating data information to a target device such as remote device 160. For example, certain users can be restricted to certain data transfer types such as HTTP (Hypertext Transfer Protocol) or FTP (File Transfer Protocol). Thus, data flow control unit 130 can be used to allow users to transmit and receive data information based on allowed session-types.

Data flows can also be regulated based on the time of day. For example, selected users can transmit and receive data only during certain work hours according to data flow rules 140, while others can transmit and receive information through data flow control unit 130 at any time. Thus, according to the principles of the present invention, it is possible to restrict an employee from accessing information on the Internet during a particular time of day. This aspect of the present invention is particularly useful in situations where an employer desires to restrict employee access of information on the Internet so that such a privilege is not abused.

A list of accessible target addresses can also be provided in data flow rules 140, indicating from which addresses information can be retrieved. This is sometimes referred to as a "white" list.

In the alternative, a list of inaccessible target addresses can be provided indicating addresses from which information can not be retrieved. This is sometimes referred to as a "black" list. Some situations require an inaccessible target list in data flow rules 140 because the accessible target list might otherwise be too large.

According to such data flow rules 140, certain users otherwise can be allowed different levels of access to target addresses such as web sites on the Internet. Such lists can change on daily basis. For example, if it is learned by a network administrator that an employee visits a web site not related to work, such a site address can be added to the black list.

One method of regulating information directed to a target address as previously discussed involves intercepting the data information packets as they are received at communication controller 136. The packets are then decoded to determine a URL address to which the data packet is directed. This is achieved by comparing the text string of the URL address with the allowed or disallowed site list for a user or group of users. If the data information includes a request for access of information that is allowed based on data flow rules 140 as selected by a key 132 in lock assembly 133, the data information including the request is further transmitted to a target destination. Consequently, it is possible to limit access of a user generating the data information

from accessing web site information on a network 150 such as the Internet.

Data flow control unit 130 and, more specifically, communication controller 136 can also decode data information packets to determine an encoded binary address to which data information is directed. For example, the data information can include an IP (Internet Protocol) destination address to which the information is directed. In a similar manner as described above, the communication controller 136 compares the IP address of data information packets to the allowed target list in data flow rules 140 to determine whether to further transmit the message or data information to an intended target destination.

A list of allowed or disallowed target destination addresses is preferably listed for each user or terminal. However, user or terminal types can be classified into groups so that data flows from a corresponding group of users or terminals is regulated according to a group-type instead of individual user or terminal-type. To support this feature, the generated data information can include information indicating from which group data information is being transmitted. Alternatively, a separate message can be sent to the data flow control unit 130 indicating from which group-type data information is generated.

Also according to the principles of the present invention, certain transmissions such as E-mail messages can be regulated so that they are not delivered to a target address. In a reverse manner, E-mail messages can be blocked from a particular user based on an address of the party generating the E-mail. This feature of the present invention is particularly beneficial to employers that desire to restrict employees who abuse the privilege

of using, for example, the Internet for communicating personal E-mail messages during work hours.

Data flows can also be regulated based on a password provided by a user or terminal generating the data information to be transmitted to a target address. As shown in Fig. 3, different users can be assigned different passwords. If the wrong password is provided by a party attempting to transmit the data information, data information from the user or terminal device 110 is potentially blocked from further transmission to a target address depending on data flow rules 140.

Fig. 4 is a diagram illustrating another application exploiting features of data flow control unit 130 according to the principles of the present invention. As shown, each data flow control unit 130 is coupled directly to a single terminal device 110. In such an application, a user having possession of a key 132 can access or communicate with other terminal devices 110 on network 300 based upon a position of key 132 in lock assembly 133 of the corresponding data flow control unit such as 130-1.

Different keys 132 can be cut so that different users at a particular terminal 110 have limited access to a network based on a corresponding type of key 132 in their possession. That is, each key 132 can be cut so that only certain data flows modes are selectable by a particular key-holder. For example, one key 132 can be cut so that only mode A or B can be selected by a key-holder. A second key can be cut so that mode A, B, or C can be selected, and so on. In this way, access to information on a network can be restricted at terminal device 110 based on a key-type that is used to select a specific data flow mode. As previously discussed, data flow can be

restricted in either direction. This aspect of the present invention is particularly useful in situations where a terminal device 110 is used by multiple users, each requiring a different level of access to a network 300 such as a LAN (Local Area Network) or WAN (Wide Area Network).

Fig. 5 is a flow chart illustrating how a data flow can be regulated according to the principles of the present invention.

Data information transmitted to communication controller 136 is intercepted in step 510. Based on a content of the data information, it is determined whether the intercepted data information shall be further transmitted to a target address. This involves retrieving key position information to determine a selected operational mode of the data flow control unit 130 in step 520.

If lock assembly 133 is in an unlocked position in step 525, the data information is transmitted to a target address on the network in step 550. Alternatively, if the lock assembly 133 is in a locked position as determined in step 525, the data information is decoded and compared to selected data flow rules 140 in step 535.

If the user requesting access is not restricted according to a selected set of data flow rules 140 as determined by a position of the key 132 in lock assembly 133 in step 540, the data information is transmitted to the corresponding target device in step 550. If the user is restricted based on a selected set of data flow rules 140 in step 540, the data information is blocked from further transmissions to the target destination in step 545 and the user is notified accordingly. Events

corresponding to blocked data transmissions or data re-transmission are optionally logged so that a system administrator can review them at a later time. It is thus possible to determine if an employee is attempting to use the system in a way that is not authorized.

While this invention has been particularly shown and described with references to preferred embodiments thereof, it will be understood by those skilled in the art that various changes in form and details may be made therein without departing from the scope of the invention encompassed by the appended claims.